IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method of detecting a malware comprising the steps of:

interrupting execution of a process that has been loaded for execution, wherein the execution of the process is interrupted by an anti-malware program;

scanning the process for a malware;

allowing the process to execute, if no malware is found; and

terminating execution of the process, if a malware is found;

wherein execution of the process comprises the step of:

loading code for execution by the process from a compressed, packed, or encrypted file;

wherein the step of interrupting execution of the process comprises the step of:

interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking, after decryption, decompression, or unpacking, where encryption, compression, or packing is carried out by an entity separate from the anti-malware program;

wherein the at least one file is selected from the group consisting of a system library file, an executable file not related to the process, and a data file not related to the process.

2. (Original) The method of claim 1, wherein the process is associated with an application program.

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Currently Amended) The method of claim [5]1, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [a]the system library file.

7. (Currently Amended) The method of claim [5]1, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [an]the executable file not related to the process.

8. (Currently Amended) The method of claim [5]1, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [a]the data file not related to the process.

9. (Currently Amended) The method of claim [5]1, wherein the malware is a computer virus.

10. (Currently Amended) The method of claim [5]1, wherein the malware is a computer worm.

11. (Currently Amended) The method of claim [5]1, wherein the malware is a Trojan horse program.

12. (Currently Amended) The method of claim [5]1, further comprising the step of:

scanning the process for a malware before execution of the process.

13. (Currently Amended) A system for detecting a malware comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

interrupting execution of a process that has been loaded for execution, wherein the execution of the process is interrupted by an anti-malware program;

scanning the process for a malware;

allowing the process to execute, if no malware is found; and

terminating execution of the process, if a malware is found;

wherein execution of the process comprises the step of:

loading code for execution by the process from a compressed, packed, or encrypted file;

wherein the step of interrupting execution of the process comprises the step of:

interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking, after decryption, decompression, or unpacking, where encryption, compression, or packing is carried out by an entity separate from the anti-malware program;

wherein the at least one file is selected from the group consisting of a system library file, an executable file not related to the process, and a data file not related to the process.

14. (Original) The system of claim 13, wherein the process is associated with an application program.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Currently Amended) The system of claim [17]13, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [a]the system library file.

19. (Currently Amended) The system of claim [17]13, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [an]the executable file not related to the process.

20. (Currently Amended) The system of claim [17]13, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [a]the data file not related to the process.

21. (Currently Amended) The system of claim [17]13, wherein the malware is a computer virus.

22. (Currently Amended) The system of claim [17]13, wherein the malware is a computer worm.

23. (Currently Amended) The system of claim [17]13, wherein the malware is a Trojan horse program.

24. (Currently Amended) The system of claim [17]13, further comprising the step of:

scanning the process for a malware before execution of the process.

25. (Currently Amended) A computer program product for detecting a malware comprising:

a computer readable medium;

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of:

interrupting execution of a process that has been loaded for execution, wherein the execution of the process is interrupted by an anti-malware program;

scanning the process for a malware;

allowing the process to execute, if no malware is found; and

terminating execution of the process, if a malware is found;

wherein execution of the process comprises the step of:

loading code for execution by the process from a compressed, packed or encrypted file;

wherein the step of interrupting execution of the process comprises the step of:

interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking, after decryption, decompression, or unpacking, where encryption, compression, or packing is carried out by an entity separate from the anti-malware program;

wherein the at least one file is selected from the group consisting of a system library file, an executable file not related to the process, and a data file not related to the process.

26. (Original) The computer program product of claim 25, wherein the process is associated with an application program.

27. (Cancelled)

28. (Cancelled)

29. (Cancelled)

30. (Currently Amended) The computer program product of claim [29]25, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [a]the system library file.

31. (Currently Amended) The computer program product of claim [29]25, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [an]the executable file not related to the process.

32. (Currently Amended) The computer program product of claim [29]25, wherein the at least one file that is not needed to perform the decryption, decompression, or unpacking comprises [a]the data file not related to the process.

33. (Currently Amended) The computer program product of claim [29]25, wherein the malware is a computer virus.

34. (Currently Amended) The computer program product of claim [29]25, wherein the malware is a computer worm.

35. (Currently Amended) The computer program product of claim [29]25, wherein the malware is a Trojan horse program.

36. (Currently Amended) The computer program product of claim [29]25, further comprising the step of:

scanning the process for a malware before execution of the process.

37. (New) The method of claim 12, further comprising the steps of:

terminating the process if malware is found before the execution of the process.

38. (New) The method of claim 37, wherein the terminating further comprises the step of:

performing anti-virus processing on the process if malware is found;

wherein the anti-virus processing includes at least one of quarantining, cleaning, and deleting files storing the loaded code.

39. (New) The method of claim 1, wherein the interrupting of the execution of the process is performed before any malware in the loaded code has a chance to perform any malicious or unauthorized actions.